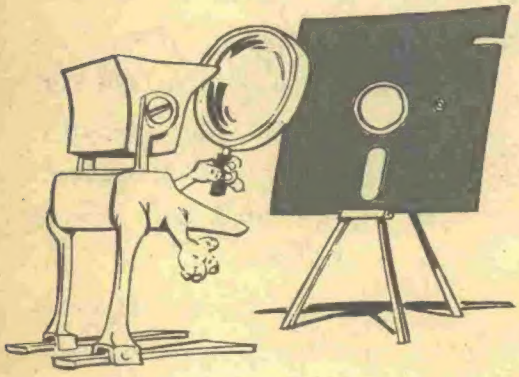
บทวิเคราะห์ ไวรัสคอมพิวเตอร์



ศ.ดร. ศรีศักดิ์ จามรมาน*

คำนำ

ใคร ๆ ก็พูดกันเรื่องไวรัสคอมพิวเตอร์ แต่หลาย ๆ คนก็พูดคนละเรื่องเดียวกัน เช่นหนังสือพิมพ์ยักษ์ใหญ่ฉบับหนึ่งบอกว่าวิธีแก้ไวรัสคอมพิวเตอร์คือถอดชิ้นส่วนคอมพิวเตอร์ออกมาเอาแอลกอฮอล์เช็ดฆ่าเชื้อไวรัส สงสัยจะไม่ใช่ไวรัสคอมพิวเตอร์อย่างที่นักคอมพิวเตอร์เขาพูดกันแล้วนะครับ คงจะเป็นไวรัสอย่างอื่นที่เผอิญมาเปรอะเปื้อนชิ้นส่วนคอมพิวเตอร์เข้า บางคนก็บอกว่า "อ๋อ ฉันรู้จักดี ไอ้ไวรัสคอมพิวเตอร์น่ะ ได้ยินใครเขาพูดกันหลายครั้งแล้ว แต่ขอกระซิบหน่อยนะ ฉันยังไม่เข้าใจเลยว่ามันคืออะไรกันแน่" บางคนก็บอกว่า "ฉันนึกว่าหน่วยงานของฉันวางมาตรการป้องกันไว้อย่างดีแล้วเชียวนะ แต่ไหงโดนไวรัสลงได้ก็ไม่ทราบ" อีกคนหนึ่งก็บอกว่า "หน่วยงานของฉันไม่มีงบประมาณเหลือที่จะมาส่งคนไปฝึกอบรมเรื่องไวรัส หรือซื้อโปรแกรมมาแก้ไวรัสหรอก แต่เราก็ใช้โปรแกรมดี ๆ ที่ไม่มีไวรัสเท่านั้น" อีก 3-4 เดือนต่อมา หน่วยงานนี้อาจจะพบไวรัสก็ได้ เพราะมีไวรัสคอมพิวเตอร์บางประเภทฟักตัวอยู่นานกว่าจะออกมาอาละวาด

สรุปแล้วรู้สึกจะพูดคนละเรื่องเดียวกัน ฉะนั้นในบทความนี้จะได้ให้คำจำกัดความของไวรัสคอมพิวเตอร์เทียบกับโปรแกรมเจ้าปัญหาอื่น ๆ วิเคราะห์ส่วนประกอบและลักษณะของไวรัสคอมพิวเตอร์ วิเคราะห์ประเภทไวรัสคอมพิวเตอร์ ให้ตัวอย่างไวรัสคอมพิวเตอร์ วิเคราะห์ว่าไวรัสเข้าคอมพิวเตอร์ได้อย่างไร เสนอรายชื่อโปรแกรมแก้ไวรัส และเสนอมาตรการอื่น ๆ ในการแก้ปัญหาไวรัสคอมพิวเตอร์

คำจำกัดความ

จากบทความเรื่อง "ทฤษฎีและการทดลองเกี่ยวกับไวรัสคอมพิวเตอร์" โดย เฟรด โคเฮน ซึ่งตีพิมพ์ในวารสารคอมพิวเตอร์และความปลอดภัย (Com-

* ผู้อำนวยการศูนย์วิจัยและพัฒนาปัญญาประดิษฐ์และซอฟต์แวร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และประธานคณะกรรมการบัณฑิตวิทยาลัยระบบสารสนเทศคอมพิวเตอร์เอแบค

puter and Security) ปีที่ 6 ฉบับที่ 1 กุมภาพันธ์ 2530 เสนอคำจำกัดความไวรัสคอมพิวเตอร์คือ "โปรแกรมที่สามารถทำให้โปรแกรมอื่นติดเชื้อได้ โดยเชื้อที่ติดนั้นคือ โปรแกรมไวรัส หรือส่วนหนึ่งของโปรแกรมไวรัส หรือโปรแกรมใหม่ที่โปรแกรมไวรัสจัดทำขึ้น และโปรแกรมที่ติดเชื้อไปนั้นสามารถทำหน้าที่เป็นพาหะของเชื้อ ทำให้สามารถแพร่เชื้อต่อไปได้"

ฉะนั้น ไวรัสคอมพิวเตอร์ ก็คือโปรแกรมคอมพิวเตอร์ประเภทหนึ่งซึ่งอาจจะแอบแฝงอยู่ในโปรแกรมอื่น ๆ อาทิ แอบแฝงอยู่ในโปรแกรมปฏิบัติการของเครื่องหรือโอเอส เป็นต้น หรือแอบแฝงอยู่ในโปรแกรมใช้งานร่วม เช่น โปรแกรมเรียงลำดับข้อมูล เป็นต้น หรือแอบแฝงอยู่ในโปรแกรมใช้งาน เช่น โปรแกรมสำหรับทำบัญชี เป็นต้น หรือแอบแฝงอยู่ในโปรแกรมเล่นเกม นั่นคือโปรแกรมไวรัสอาจจะแอบแฝงอยู่ในโปรแกรมใดก็ได้ คงเหมือนโรคเอดส์นะครับ อุปมาเห็นสาว ๆ สวย ๆ หรือหนุ่ม ๆ หล่อ ๆ สมัยนี้ อย่าไว้ใจว่าจะไม่มีเอดส์ ฉันใด อุปมัยเห็นโปรแกรมดี ๆ ก็อย่าไว้ใจว่าจะไม่มีเชื้อไวรัส ฉันนั้น

ไวรัสแตกต่างจากโปรแกรมเจ้าปัญหาแบบอื่น

บางท่านอาจจะรวมไวรัสไว้ในบรรดาโปรแกรมที่ก่อให้เกิดปัญหาโปรแกรมอื่น ๆ แต่วงการผู้เชี่ยวชาญไวรัสคอมพิวเตอร์ในสหรัฐอเมริกาเสนอให้แยกไวรัสเป็นประเภทของตัวมันเอง แตกต่างจากโปรแกรมเจ้าปัญหาอื่น ๆ คือ โปรแกรมประตูกล โปรแกรมม้าอารีย์ โปรแกรมหนอนบ้าอำนาจ และโปรแกรมระเบิดเวลา

โปรแกรมประตูกล

คือส่วนหนึ่งของโปรแกรมที่ผู้พัฒนาโปรแกรมจัดทำไว้เพื่อความสะดวกในการเข้าไปปรับปรุงแก้ไขโปรแกรม โดยไม่ต้องเป็นห่วงเรื่องรหัสผ่าน โปรแกรมประตูกลนี้มีใช้กันในโปรแกรมที่จำเป็นต้องมีการป้องกันอย่างดี กว่าผู้ใช้จะเข้าไปใช้ได้ก็ต้องบอกรหัสผ่านซึ่งอาจจะเปลี่ยนแปลงไปได้ทุกครั้งที่เลิกใช้ นั่นคือ ถ้าใครบอกรหัสผ่านได้ถูกต้องเวลาจะเข้าไปใช้ เมื่อใช้เสร็จแล้วถึงเวลา

จะเลิก โปรแกรมก็จะถามว่าจะเปลี่ยนรหัสผ่านหรือไม่ ถ้าเปลี่ยนเป็นรหัสใหม่อย่างไรแล้วเวลาใครจะมาใช้ครั้งต่อไปจะต้องบอกรหัสใหม่นั้นให้ได้ ถ้าบอกรหัสใหม่ไม่ได้ก็เข้าไม่ได้ ทีนี้ก็มีปัญหาว่า คนที่เปลี่ยนรหัสใหม่แล้วตัวเองจำไอ้รหัสนั้นไม่ได้ จะใช้ก็ไม่ได้แล้วจะทำอะไรก็ไม่ได้ ฉะนั้นเวลาสร้างโปรแกรมในตอนแรก ผู้สร้างโปรแกรมเขาก็เลยจัดทำประตูกลไว้สำหรับตัวเขาเอง หรือสำหรับเจ้าหน้าที่ศูนย์คอมพิวเตอร์จะได้สามารถใช้ประตูกลนี้เข้าไปได้โดยไม่ต้องใช้รหัสผ่าน เมื่อเข้าไปได้แล้วก็ออกมาโดยตั้งรหัสใหม่หรือไม่ตั้งก็ได้ นอกจากจะแก้ปัญหาเรื่องการจำรหัสไม่ได้แล้ว ประตูกลนี้ยังสามารถใช้ได้ในการเข้าไปแก้โปรแกรมที่ต้องการแก้ ตัวอย่างของประตูกลก็มีในภาพยนตร์เรื่อง วอร์เกมส์ (War Games) ซึ่งใช้คำว่า "โจชัว" (Joshua) ก็เข้าโปรแกรมได้

นอกจากจะมีประตูกลทางซอฟต์แวร์แล้ว ก็อาจจะไปทำประตูกลทางฮาร์ดแวร์ได้ เช่นในเครื่องไอบีเอ็ม/พีเอสทู มีประตูกลใช้ช่างเข้าไปในโปรแกรมได้โดยต่อสายสวิตช์สองเส้นเข้าด้วยกัน แล้วไม่ต้องบอกรหัสผ่านและเลขที่บัญชีก็เข้าโปรแกรมได้

โปรแกรมม้าอารีย์

โปรแกรมนี้ได้ชื่อมาจากเรื่องม้าอารีย์ในสมัยโบราณ ที่มีข้าศึกยกกองทัพเรือมารบกันอยู่นาน แล้ววันดีคืนดีก็เอาม้าไม้ตัวใหญ่มาทิ้งไว้ที่ประตูเมืองทรอย ชาวเมืองไม่ทราบว่าข้างในท้องม้ามีทหารแอบแฝงอยู่ เห็นข้าศึกถอยเรือออกไปแล้ว นึกว่าข้าศึกยอมแพ้ จึงลากจูงม้าไม้เข้าไปในเมืองเป็นที่ระลึกว่ารบชนะ พอตกดึกทหารข้าศึกก็แอบออกมาจากท้องม้า เปิดประตูเมืองให้กองทัพข้าศึกเข้าไปทำลายเมืองได้ในที่สุด ในด้านโปรแกรมก็เอาโปรแกรมข้าศึกซ่อนอยู่ในโปรแกรมดี ๆ เช่น ซ่อนในโปรแกรมใช้งาน ซ่อนในโปรแกรมใช้งานร่วม หรือ ซ่อนในโปรแกรมเล่นเกม เป็นต้น เวลาสาธิตให้ดู เจ้าโปรแกรมข้าศึกก็นอนนิ่งอยู่เฉย ๆ พอเอาโปรแกรมไปใช้เข้าจริง ไอ้เจ้าโปรแกรมข้าศึกก็จะลุกออกมาทำความเสียหายต่าง ๆ นานาในเครื่องนั้นเอง ไม่ได้ออกไปอาละวาดที่อื่น ถ้าไปอาละวาดที่อื่นด้วยจึงจะกลายเป็นโปรแกรมไวรัสไป

โปรแกรมหนอนบ้าอำนาจ

เจ้าโปรแกรมหนอนนี้เดิมเป็นหนอนที่ทรงคุณธรรมดี แต่ต่อมาภายหลังกลายเป็นหนอนบ้าอำนาจไป ตอนแรก ๆ นั้นคนเขียนโปรแกรมหนอนคนแรกต้องการจะใช้เครื่องคอมพิวเตอร์ให้ได้ประสิทธิภาพมากที่สุด จึงจัดทำโปรแกรมหนอนขึ้นเพื่อคลานเข้าไปดูว่าเวลามีโปรแกรมพระเอกเขาใช้งานคอมพิวเตอร์อยู่นั้น มีส่วนไหนของคอมพิวเตอร์ว่างบ้าง ถ้าพบเจ้าหนอนก็แอบเอาโปรแกรมพระรองที่รอคิวอยู่เข้าไปทำงานโดยไม่ให้เสียงานของโปรแกรมพระเอก ฉะนั้นผลสุดท้ายในระหว่างที่ทำงานพระเอกไปก็ได้ทำงานพระรองไปด้วย ทำให้ได้ประสิทธิภาพมากขึ้น แต่ต่อมาเจ้าของงานพระรองเกิดอิจฉางานพระเอกเลยแก้โปรแกรมหนอนให้เอางานพระรองเข้าไปทำในส่วนที่ว่างของเครื่อง แล้วจากจุดนั้นก็ยึดอำนาจขับไล่งานพระเอกออกไป ทำให้ได้ทำงานพระรองเสร็จก่อน นั่นคือ ในเครื่องที่สามารถทำงานหลายงานได้พร้อม ๆ กัน ใครอยากจะให้งานของตนเสร็จก่อนก็เอาโปรแกรมหนอนบ้าอำนาจมาใช้กับงานของตน

โปรแกรมระเบิดเวลา

โปรแกรมนี้คล้ายกับโปรแกรมม้าอารีย์ ในแง่ที่เป็นโปรแกรมแอบแฝงอยู่ในโปรแกรมอื่น และจะแอบอยู่อย่างนั้นไม่ลุกขึ้นมาทำอะไร จนได้เวลาที่ตั้งเอาไว้ล่วงหน้าเหมือนการตั้งเวลาสำหรับระเบิดเวลา เช่นเมื่อถึงวันเกิดของคนเขียนโปรแกรม เจ้าโปรแกรมก็จะลุกขึ้น

มาหยุดงานของคนอื่นทุกคน แล้วประกาศบนหน้าจอทุกจอว่า ถึงวันเกิดของผมแล้ว ขอให้ผู้ใช้เทอร์มินัลทุกคนหยุดใช้เทอร์มินัลไปซื้อเค็กที่ร้านอาหาร รับประทานเค็กฉลองวันเกิดให้ผม อีก 15 นาทีค่อยกลับมาใช้เครื่องต่อไปได้ อะไรทำนองนั้น

ส่วนประกอบของโปรแกรมไวรัส

ผู้เชี่ยวชาญไวรัสคอมพิวเตอร์ในอเมริกาตกลงกันว่า โปรแกรมไวรัสจะต้องมีส่วนประกอบ 3 ส่วน คือ

1. ส่วนคัดลอก

ส่วนคัดลอกเป็นโปรแกรมสำหรับคัดลอกตัวโปรแกรมไวรัสหรือส่วนของโปรแกรมไวรัส หรือโปรแกรมอื่นใดที่โปรแกรมไวรัสจัดทำขึ้น ลงไปอยู่ในแฟ้มอื่น โดยคัดลอกลงไปเก็บไว้เฉย ๆ ยังไม่ได้ทำอันตรายอะไร คล้าย ๆ กับเอาของใส่กล่องไปแจกเอาไว้ ผู้รับก็ไม่ทราบว่าของในกล่องนั้นคืออะไร

2. ส่วนสะกิดให้เริ่มลงมือ

เป็นโปรแกรมที่สะกิดว่าได้เวลาลงมือแล้ว โดยปลุกโปรแกรมส่วนที่สามให้ลุกขึ้นมาทำงาน ส่วนสะกิดนี้อาจจะเป็นคำสั่งตรวจสอบว่า วันที่เท่าใด เวลาใด เมื่อถึงวันที่และเวลานั้นก็จะสั่งให้ลงมือได้ หรืออาจจะตรวจสอบว่าได้ทำตามส่วนที่หนึ่งไปจนครบจำนวนครั้งที่กำหนดไว้ล่วงหน้าแล้ว เช่นไวรัสบางตัวคัดลอกครบ 4 ครั้งก็ลุกขึ้นมาปฏิบัติการโหดครั้งหนึ่ง แล้วหยุดรอจนคัดลอกครบ 4 ครั้งใหม่ก็ลุกขึ้นมาปฏิบัติการโหดอีกครั้งหนึ่ง เป็นต้น

ฉะนั้นไวรัสอาจจะสงบนิ่งอยู่เป็นเดือน หรือเป็นปีก็ได้แล้วแต่ว่าผู้สร้างไวรัสเขาจะกำหนดเอาไว้อย่างไร ฉะนั้นโปรแกรมที่เราอัดสำเนาสำรองอย่างดีอาจจะมีไวรัสแฝงอยู่โดยที่เราไม่รู้ก็ได้ แล้วพอเราเอาโปรแกรมนั้นมาใช้สักพักหนึ่งจึงเกิดเรื่องขึ้นได้

3. ส่วนปฏิบัติการโหด

ส่วนที่สามหรือส่วนปฏิบัติการโหดก็เป็นโปรแกรมส่วนที่ลงมือปฏิบัติการซึ่งขึ้นอยู่กับความต้องการของผู้สร้างไวรัสว่าจะโหดเพียงใด ไวรัสบางตัวอาจจะไม่โหดมาก คือใช้โปรแกรมส่วนที่สามนี้แสดงข้อความบนจอ ให้ผู้ใช้รำคาญเล่นเท่านั้น แต่ไวรัสบางตัวก็อาจจะโหดมากโดยใช้โปรแกรมส่วนที่สามนี้ไปลบโปรแกรมอื่น หรือลบข้อมูลออกมากบ้างน้อยบ้าง หรือไปคัดลอกส่วนหนึ่งของโปรแกรมใดโปรแกรมหนึ่งไปไว้ยังอีกส่วนหนึ่ง ทำให้โปรแกรมหรือข้อมูลค่อย ๆ หายไปทีละน้อย หรือค่อย ๆ เพิ่มขึ้นทีละน้อย จนผิดไปทั้งหมดในที่สุดก็ได้

มีอยู่ระยะหนึ่งมีการใช้คำว่าหนอนและมะเร็งแสดงประเภทของไวรัส ถ้าเป็นไวรัสที่ไปลบโปรแกรมหรือข้อมูลอื่นทีละน้อยก็เรียกว่าเป็นไวรัสประเภทหนอน ทำนองเดียวกับหนอนที่เจาะไชใบไม้ หรือผลไม้ไปทีละน้อย ถ้าเป็นไวรัสที่ไปคัดลอกโปรแกรมหรือข้อมูลซ้ำ ๆ กันให้เพิ่มพูนกินเนื้อที่ส่วนความจำมากขึ้นเรื่อย ๆ ก็อาจกล่าวได้ว่าไวรัสนั้นเป็นไวรัสประเภทมะเร็ง ในทำนองเดียวกับที่มะเร็งมีเนื้อร้ายขยายตัวของมันเองมากขึ้นเรื่อย ๆ

ตัวอย่างวิธีสร้างไวรัส

มีตัวอย่างกรณีไวรัสคอมพิวเตอร์ในอเมริกามากมายหลายตัวอย่าง กล่าวกันว่าถ้าท่านเป็นนักคอมพิวเตอร์ ท่านจะสามารถสร้างไวรัสใหม่ได้ภายในหนึ่งวัน ถ้าท่านไม่ได้เป็นนักคอมพิวเตอร์ ท่านจะสามารถศึกษาหาความรู้โดยอ่านจากเอกสารต่าง ๆ แล้วนำความรู้นั้นมาสร้างไวรัสใหม่ได้ภายใน 1 เดือน

เมื่อเดือนกรกฎาคม 2529 วารสารคอมพิวเตอร์แฮกเกอร์ ตีพิมพ์ตัวอย่างโปรแกรมไวรัสสำหรับใช้กับเครื่อง DEC พร้อมทั้งคำอธิบายวิธีสร้างไวรัสใหม่ ๆ สำหรับเครื่องนี้ ให้ผู้อ่านไปสร้างเล่นได้

ไวรัสคอมมอดอร์อามิกา (Commodore Amiga)

เมื่อเดือนพฤศจิกายน 2530 ผู้ที่ซื้อโปรแกรมจากคอมมอดอร์คอมพิวเตอร์ทั้งในอเมริกา อังกฤษ และออสเตรเลีย พบว่าโปรแกรมที่ซื้อไปนั้น พอจะใช้ก็แสดงบนจอว่าไม่ให้ใช้ ปรากฏว่ามีมือดีเอาไวรัสใส่ในโปรแกรมต้นฉบับของคอมมอดอร์ เมื่อคอมมอดอร์คัดลอกโปรแกรมนั้นไปขายก็ติดไวรัสไปด้วย เป็นตัวอย่างที่แสดงให้เห็นว่าขนาดโปรแกรมที่ซื้อมาโดยตรงจากผู้ผลิตก็อาจมีไวรัสติดมาด้วยได้ แต่ยังโชคดีที่มือดีนั้นทำไวรัสแบบง่าย ๆ ไม่ได้ทำความเสียหายมาก

ไวรัสเลไฮ (Lehigh)

เมื่อเดือนพฤศจิกายน 2530 เช่นกัน มหาวิทยาลัยเลไฮในอเมริกาพบไวรัสในโปรแกรมปฏิบัติงานของเครื่อง หรือโอเอส เวลาใช้โอเอสครั้งใด เจ้าไวรัสก็ลุกขึ้นมาคัดลอกตัวเองครั้งหนึ่ง เมื่อคัดลอกครบ 4 ครั้ง มันก็ลุกขึ้นมาลบโปรแกรมหรือข้อมูลของชาวบ้านเล่นตามชอบใจ เมื่อเกิดปัญหาข้อมูลหายและโปรแกรมไม่ทำงานหลาย ๆ ครั้งเข้า เจ้าหน้าที่ศูนย์คอมพิวเตอร์จึงค้นหาสาเหตุและจัดการลบไวรัสตัวนี้ได้

ไวรัสคริสต์มาสไอบีเอ็ม

เมื่อเดือนธันวาคม 2530 ระบบไปรษณีย์อิเล็กทรอนิกส์ของไอบีเอ็มถูก

ไวรัสตัวนี้บุก โดยเจ้าไวรัสตัวนี้จะแสดงรูปต้นคริสต์มาสบนจอ แล้วคัดลอกตัวเองลงในแฟ้มไปรษณีย์อิเล็กทรอนิกส์ของทุกคนที่ใช้บริการ กลายเป็นจดหมายแบบลูกโซ่ (Chain Letter) เดี๋ยวเดียวก็กินที่เต็มหมด ช่างของไอบีเอ็มต้องปิดเครื่องและปิดบริการไปรษณีย์อิเล็กทรอนิกส์ ค้นหาสาเหตุจนพบ แล้วจัดการลบไวรัสตัวนี้ออก

ไวรัสมหาวิทยาลัยฮีบรู (Hebrew)

เมื่อเดือนมกราคม 2531 เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยฮีบรูทำงานช้าลงมาก จึงมีการค้นหาสาเหตุ จนพบไวรัสตัวนี้ ซึ่งจะคัดลอกตัวเองลงแฟ้มข้อมูลทุกแฟ้ม และคัดลอกต่อไปเรื่อย ๆ ทำให้แฟ้มเต็มหมด งานต่าง ๆ จึงช้าลง ปรากฏว่าส่วนสะกิดให้ลงมือของไวรัสตัวนี้ คือรอให้ถึงวันศุกร์ที่ 13 เดือนพฤษภาคม 2531 จึงลุกขึ้นมาลบแฟ้มข้อมูลทั้งหมด โชคดีที่พบเสียก่อนวันศุกร์ที่ 13 นั้น

ไวรัสสันติภาพ (Peace)

เมื่อเดือนมีนาคม 2531 มีการค้นพบไวรัสในจานแม่เหล็กเป็นพัน ๆ แผ่น ที่บรรจุโปรแกรมของบริษัทอาร์ดิสในเมืองซีแอตเทิล ไวรัสตัวนี้ไม่ทำอันตรายอะไรมาก นอกจากแสดงข้อความบนจอส่งเสริมสันติภาพเท่านั้น และต่อมาก็มีผู้พบไวรัสตัวนี้ ในบริการประกาศ (Bulletin Board) ของบริษัทคอมพิวเซิร์ฟ (Compuserve) และบริษัท จีอี (GE)

ไวรัสเบรน (Brain)

ระหว่าง พ.ศ. 2530-2531 มหาวิทยาลัยต่าง ๆ เช่น จอร์จวอชิงตัน พิตสเบิร์ก เพนซิลเวเนีย และเวอร์จิเนียร์ พบไวรัสที่ไปเปลี่ยนชื่อจานแม่เหล็กเป็นชื่อ "เบรน (BRAIN)" โดยที่ไวรัสตัวนี้จะคัดลอกตัวเองลงในส่วนหนึ่งของจานแม่เหล็ก เป็นการลบโปรแกรมหรือข้อมูลที่มีอยู่ในส่วนนั้นของจานแม่เหล็ก พอถึงเวลาไวรัสตัวนี้ก็ลุกขึ้นมาประกาศ ชื่อ ที่อยู่ และหมายเลขโทรศัพท์ ของผู้สร้าง ซึ่งอยู่ในปากีสถาน และบางทีก็บอกให้ส่งเงินไปให้ ถ้าอยากจะทราบว่าจะแก้ไขอย่างไร

ไวรัสสกอร์ (Scores)

พบระหว่างเดือนธันวาคมถึงเมษายน 2531 โดยหน่วยงานรัฐบาลอเมริกัน อาทิ รัฐสภา ที่ใช้เครื่องคอมพิวเตอร์ยี่ห้อแอปเปิ้ลแมคอินทอช โดยเจ้าไวรัสตัวนี้จะคัดลอกรูปแบบต่าง ๆ ของตัวมันเอง 3 แบบ ลงบนแฟ้มต่าง ๆ 4 แฟ้ม รวมเป็น 12 ชุด เมื่อพบครั้งใดแล้วก็ต้องลบออกทั้ง 12 ชุด

ไวรัสปลอมเป็นโปรแกรมแก้ไวรัส

จากการที่มีไวรัสระบาดก็มีผู้จัดทำโปรแกรมแก้ไวรัสออกจำหน่ายจ่ายแจกกันมากมาย โปรแกรมแก้ไวรัสโปรแกรมหนึ่งชื่อ ฟลูชอร์ตที่สาม (Flu-Shot 3) หรือยาฉีดชุดที่สามสำหรับแก้ไข้หวัด ต่อมามีนักสร้างไวรัสจัดทำไวรัสโดยตั้งชื่อว่า ฟลูชอร์ตที่สี่ (Flu-Shot 4) ทำให้คนเข้าใจผิดคิดว่าเป็นฉบับปรับปรุงแก้ไขของฟลูชอร์ตที่สาม แต่ความจริงแล้วเป็นไวรัสที่อาละวาดโดยลบแฟ้มทั้งในฟลอปปี้ดิสก์และฮาร์ดดิสก์

พาหะแพร่เชื้อไวรัส

พาหะที่สำคัญแยกได้เป็น 3 ประเภท คือ

1. สื่อเก็บโปรแกรม

ในกรณีของสื่อเก็บโปรแกรมไม่ว่าจะเป็นแผ่นดิสเกตต์หรือเทปตลับ หรือเทปม้วนใหญ่หรือดิสค์แพค หรือสื่ออื่นใด ถ้ามีไวรัสอยู่ในโปรแกรมใดในสื่อนั้น เมื่อนำสื่อนั้นไปใช้กับเครื่องใดแล้วเรียกใช้โปรแกรมที่มีเชื้อไวรัสอยู่ เชื้อไวรัสนั้นจะแพร่ขยายได้ทันที

2. เครือข่ายคอมพิวเตอร์

ในกรณีของเครือข่ายคอมพิวเตอร์ไม่ว่าจะเป็นเครือข่ายท้องถิ่นที่เรียกว่า แลน (LAN = LOCAL AREA NETWORK) หรือเครือข่ายที่ต้องใช้โมเด็ม ไม่ว่าจะเป็นเครื่องไมโครหรือมินิหรือเมนเฟรม เมื่อมีการใช้โปรแกรมที่มีไวรัสจากเทอร์มินัลใด เจ้าไวรัสก็จะลุกขึ้นจากเทอร์มินัลนั้นใช้เครือข่ายเป็นพาหะแพร่เชื้อไปยังเทอร์มินัลอื่น หรือคอมพิวเตอร์อื่นได้

3. โปรแกรมปฏิบัติการของเครื่อง

ในกรณีของโปรแกรมปฏิบัติการอาจจะมีไวรัสอยู่ในส่วนของโปรแกรมที่ชื่อว่า บูตเซกเตอร์ (BOOT SECTOR) หรือโปรแกรมสำหรับเรียกโปรแกรมส่วนอื่น ๆ ถ้ามีไวรัสอยู่ในบูตเซกเตอร์ก็นับได้ว่าบูตเซกเตอร์เป็นพาหะ ไวรัสจะลุกขึ้นมาอาละวาดได้ทันทีที่ใช้บูตเซกเตอร์นั้นเมื่อตอนเปิดเครื่อง

ในอีกแง่หนึ่งก็จะวิเคราะห์ว่าไวรัสเข้าคอมพิวเตอร์ได้อย่างไรก็อาจจะสรุปได้เป็น 2 วิธีคือ

วิธีที่หนึ่ง โดยการเขียนและพิมพ์โปรแกรมใส่เข้าไปในโปรแกรมอื่นโดยตรง

วิธีที่สอง ซึ่งเป็นวิธีที่เกิดมากที่สุดคือ โดยการใช้โปรแกรมที่เราไม่ทราบ

ว่ามีไวรัส แล้วเจ้าไวรัสก็จัดการคัดลอกตัวเองลงในโปรแกรมอื่น ๆ

การใช้โปรแกรมที่มีไวรัส แม้แต่เพียงครั้งเดียวเท่านั้น เจ้าไวรัสนั้นก็จะคัดลอกตัวเองลงในโปรแกรมอื่น ฉะนั้นถ้ามองในแง่นี้ไวรัสคอมพิวเตอร์ก็อาจจะร้ายกว่าเอดส์ก็ได้ เพราะการมีเพศสัมพันธ์กับคนที่มีเชื้อเอดส์เพียงครั้งเดียวอาจจะติดหรือไม่ติดก็ได้ แต่การใช้โปรแกรมที่มีไวรัสคอมพิวเตอร์เพียงครั้งเดียวก็รับรองว่ามีการแพร่ไวรัสคอมพิวเตอร์แน่ ๆ ยิ่งกว่านั้นถ้าไวรัสคอมพิวเตอร์เข้าถึงโอเอสเมื่อไรมันก็จะมีอำนาจมากขึ้นกว่าตอนที่อยู่ในโปรแกรมใช้งานธรรมดา นั่นคือถ้าอยู่ในโปรแกรมใช้งานธรรมดามันก็แพร่เชื้อให้ได้เฉพาะโปรแกรมในระดับเดียวกัน แต่ถ้าเผอิญโอเอสเกิดมาเรียกใช้โปรแกรมธรรมดาที่มีไวรัสอยู่แล้ว โอเอสติดไวรัสไป โอเอสก็จะเอาเชื้อนี้ไปแพร่ให้โปรแกรมอื่น ๆ ได้อีกมากมาย เพราะโอเอสเป็นโปรแกรมระดับสูงกว่าโปรแกรมธรรมดา

โดยสรุปแล้ว จากแหล่งเดียวเจ้าไวรัสอาจแพร่หลายออกรวดเร็วจนระบบคอมพิวเตอร์ที่มีเครื่องเชื่อมโยงเป็นพัน ๆ เครื่อง ถูกไวรัสมากมายจนทำงานต่อไปไม่ได้ภายในเวลาเป็นนาทีหรือชั่วโมงก็ได้

ถ้าเรามีเทอร์มินัลตัวหนึ่งต่อเข้ากับคอมพิวเตอร์ใหญ่ระบบหนึ่ง แล้วติดไวรัสจากระบบนั้นมาเข้าดิสเกตต์ของเทอร์มินัล พอเราเอาเทอร์มินัลตัวนั้นมาต่อกับคอมพิวเตอร์ในอีกระบบหนึ่ง เจ้าไวรัสจากดิสเกตต์ของเทอร์มินัลก็อาจจะแพร่เข้าไปในคอมพิวเตอร์ใหญ่ในอีกระบบนั้นได้ด้วย

ปกติเครื่องไมโครคอมพิวเตอร์ในหน่วยงานต่าง ๆ มักจะให้ผู้ใช้หลาย ๆ คนใช้ร่วมกันได้ เช่นตามมหาวิทยาลัย วันหนึ่ง ๆ อาจจะมีคนใช้ไมโครเครื่องใดเครื่องหนึ่งถึง 20 คน ฉะนั้นไวรัสจากผู้ใช้คนแรกอาจจะแพร่เชื้อไปให้อีก 19 คนได้ภายในหนึ่งวัน

ยิ่งกว่านั้นตามมหาวิทยาลัยมักจะมีห้องสมุดซอฟต์แวร์ ให้นักศึกษายืมแฟ้มซอฟต์แวร์ในดิสเกตต์ไปใช้ได้ ถ้านักศึกษาคนใดยืมซอฟต์แวร์ที่ไม่มีเชื้อไวรัสไปใช้กับเครื่องไมโครที่มีไวรัสอยู่ในฮาร์ดดิสก์ ทำให้ซอฟต์แวร์ในแผ่นดิสเกตต์ติดไวรัสมา พอนักศึกษามาอีกคนหนึ่งยืมแผ่นดิสเกตต์ที่มีไวรัสอยู่ไปใช้กับอีกเครื่องหนึ่งที่ไม่มีเชื้อไวรัส ไวรัสจากดิสเกตต์ก็ไปติดเครื่องใหม่แพร่ขยายตัวไปได้อย่างรวดเร็ว

ประเภทไวรัสคอมพิวเตอร์

ในทำนองเดียวกับไวรัสทางชีววิทยา เราอาจจะวิเคราะห์แบ่งประเภทไวรัสคอมพิวเตอร์ได้ โดยที่ในอเมริกาเขาก็แบ่งประเภทไวรัสเป็น 4 ประเภท คือ

1. ไวรัสเกาะรอบนอก

ประเภทที่หนึ่งคือ ไวรัสเกาะรอบนอกนั้น เวลาคัดลอกลงในโปรแกรมใดจะไปอยู่ด้านนอกคือ ตอนต้นหรือตอนท้ายของโปรแกรมนั้น ฉะนั้นเวลาผู้ใช้เรียกใช้โปรแกรมที่มีไวรัส ตัวโปรแกรมไวรัสก็จะทำงานก่อนโปรแกรมเดิม ถ้าไวรัสอยู่ตอนต้นของโปรแกรมเดิม หรือทำงานหลังโปรแกรมเดิมถ้าไวรัสอยู่ตอนท้ายของโปรแกรมเดิม นั่นคือทุกครั้งที่เรียกใช้โปรแกรมใช้งานหนึ่งครั้ง โปรแกรมไวรัสก็จะทำงานหนึ่งครั้ง การทำงานของมันอย่างน้อยที่สุดก็คัดลอกตัวเองลงไปในโปรแกรมอื่นหนึ่งครั้ง และดูตัวสะกิดว่าถึงกำหนดให้ปฏิบัติการโหดของมันต่อหรือไม่ ถ้าถึงแล้วก็ลงมือปฏิบัติการโหดของมัน ถ้ายังไม่ถึงเวลาก็รอไปก่อน

ไวรัสแบบที่หนึ่งนี้เป็นโปรแกรมครบถ้วนในตัวของมันเองไม่ได้เข้าไปยุ่งเกี่ยวแก้ไขอะไรในโปรแกรมใช้งานเลย ฉะนั้นโปรแกรมใช้งานก็ทำงานตามปกติทุกอย่าง ไวรัสแบบนี้จะเขียนง่าย ตรวจพบง่าย เพราะมันทำให้โปรแกรมใช้งานยาวขึ้นและมันอาจจะเปลี่ยนวันเวลาที่ระบุการแก้ไขโปรแกรมการใช้งานนั้น และเมื่อพบแล้วก็ลบออกได้ง่ายเพราะมันอยู่ตอนต้นหรือตอนท้ายของโปรแกรมใช้งานไม่ได้ไปสอดแทรกที่อื่น

2. ไวรัสเจาะไชเข้าไปข้างใน

ไวรัสแบบนี้ไม่ได้เป็นโปรแกรมครบถ้วนในตัวของมันเอง มันจะเจาะแฝงเข้าไปเป็นส่วนหนึ่งของโปรแกรมใช้งาน มันอาจจะย้ายส่วนหนึ่งของโปรแกรมใช้งานไปอยู่ตอนต้นหรือตอนท้ายของโปรแกรมใช้งานเดิม แล้วตัวของมันเองก็เข้าไปอยู่ในที่ว่างนั้น

ไวรัสแบบนี้เขียนยากและลบยาก เพราะมันจะแยกอยู่หลาย ๆ ที่ในโปรแกรมใช้งานก็ได้ แต่การตรวจพบนั้นง่ายเพราะมันมักจะทำให้โปรแกรมใช้งานยาวขึ้น และมันเปลี่ยนโครงสร้างของโปรแกรมใช้งานให้มีการกระโดดไปมามากขึ้น

3. ไวรัสในโอเอส

ไวรัสแบบนี้แอบแฝงอยู่ในโอเอส เช่น อยู่ในบูตเซกเตอร์ ทุกครั้งที่เปิดเครื่องมันก็จะลุกขึ้นมาก่อกวน ส่วนการก่อกวนก็แล้วแต่ว่าผู้สร้างได้สร้างมันให้มันก่อกวนอย่างไร ไวรัสแบบนี้เขียนยากและตรวจพบยากแต่ลบออกง่าย

4. ไวรัสตั้งแต่เกิด

ไวรัสแบบนี้ผู้สร้างใส่ไว้ในโปรแกรมใช้งานตั้งแต่ตอนสร้างโปรแกรมใช้งานหรือตอนที่โปรแกรมใช้งานถือกำเนิดเกิดขึ้น ส่วนมากมักจะเขียนด้วยภาษาแอสเซมบลีหรือภาษาซี ซึ่งทำให้สามารถก่อกวนคอมพิวเตอร์ได้หลายยี่ห้อที่ใช้ภาษาแอสเซมบลีเหมือนกันหรือยอมรับภาษาซีเหมือนกัน ถ้ามีการตรวจสอบการพัฒนาโปรแกรมอย่างละเอียดถี่ถ้วนก็อาจจะตรวจพบไวรัสตัวนี้และจัดการลบออกได้โดยง่าย แต่ถ้าตรวจไม่พบตั้งแต่ต้นก็อาจตรวจภายหลังลำบาก เพราะจะตรวจความยาวของโปรแกรมใช้งานก็ไม่ได้ เพราะมันเกิดมาจากโปรแกรมใช้งานความยาวของมันจึงรวมอยู่ในความยาวของโปรแกรมใช้งานตั้งแต่ต้น

การใช้ไวรัสให้เป็นประโยชน์

ทุกอย่างในโลกนี้ย่อมมีสองด้านอย่างเหรียญบาทก็มีหัวและมีก้อย ฉะนั้นเมื่อมีการใช้ไวรัสในทางบ่อนทำลายได้ก็น่าจะมีการใช้ไวรัสในทางสร้างสรรค์ได้ ดังตัวอย่างเช่น การใช้ไวรัสในการประหยัดที่ในแผ่นดิสเกตต์และการใช้ไวรัสป้องปรามการคัดลอกโปรแกรมโดยไม่ได้รับการอนุญาต

ในด้านการใช้ไวรัสช่วยประหยัดที่ในแผ่นดิสเกตต์นั้น ได้มีการสร้างโปรแกรมไวรัสขึ้นมาเกาะไว้ที่โปรแกรมใดโปรแกรมหนึ่ง เมื่อเรียกใช้โปรแกรมนั้นมันก็จะสำรวจตรวจหาโปรแกรมที่ไม่มีไวรัสแล้วแสดงข้อความบนจอ ขออนุญาตดำเนินการประหยัดที่สำหรับโปรแกรมนั้นให้ ตัวเจ้าของโปรแกรมยอมเจ้าไวรัสก็ไปเกาะอยู่ตอนต้นของโปรแกรมนั้น จัดการใช้รหัสย่อความยาวของโปรแกรมและข้อมูล เช่น ถ้าในข้อมูลมีคำว่า "กรุงเทพ" ซึ่งมี 7 ตัวอักษรรวมอยู่หนึ่งล้านคำ มันก็ใช้ 0 แทนคำว่า "กรุงเทพ" นั่นคือลดจากเจ็ดเป็นหนึ่งตัวทำให้สามารถลดที่ได้จากเจ็ดล้านตัวเหลือหนึ่งล้านตัว เวลาจะใช้แฟ้มข้อมูลนั้นเจ้าไวรัสจะแปลงรหัสกลับให้เป็นอย่างเก่า และเวลาเลิกใช้จะเก็บเข้าที่เก่ามันก็ย่อให้

ส่วนการใช้ไวรัสป้องปรามการคัดลอกโปรแกรมโดยไม่ได้รับการอนุญาตนั้นก็นำไวรัสไปใส่ไว้ในตอนต้นโปรแกรมที่ไม่ต้องการให้มีการคัดลอก พอใครจะคัดลอกเจ้าไวรัสก็แสดงข้อความบนจอ บอกว่าการคัดลอกนี้ผิดกฎหมาย ถ้าอยากได้สำเนาขอให้ไปซื้อได้ที่ไหน ถ้าใครยังขืนคัดลอกก็จดเอาไว้ว่าคัดลอกกี่ครั้งแล้ว และพยายามส่งข้อมูลการคัดลอกนี้กลับไปในเครือข่ายคอมพิวเตอร์ให้ไปถึงเจ้าของโปรแกรมให้ได้

ความเสียหายจากไวรัสคอมพิวเตอร์

โดยสรุปแล้วโปรแกรมไวรัสจะทำความเสียหายได้มากน้อยเพียงใดขึ้นอยู่กับว่าผู้สร้างได้สร้างไว้อย่างไร ถ้าสร้างให้แสดงข้อความบนจอเฉย ๆ ก็เพียงแต่ก่อความรำคาญไม่เสียหายอะไรนัก ถ้าสร้างให้ลบโปรแกรมและข้อมูลทั้งหมดก็อาจจะเสียหายมากถ้าไม่มีแฟ้มสำรองไว้ แต่จะดีในแง่ที่ทราบได้ทันทีว่าได้มีการโจมตีจากไวรัสแล้ว ถ้าสร้างให้ลบอะไรไปทีละนิดละหน่อยอาจจะกล่าวว่า ความเสียหายแต่ละครั้งไม่มาก แต่รวมแล้วความเสียหายอาจจะมากก็ได้

ความเสียหายทางอ้อมจากไวรัสก็คือ การเสียเงินและเวลาในการตรวจหาและแก้ไขปัญหาที่เกิดจากไวรัส

การตรวจหาอาจจะยากมาก ดังตัวอย่างในไวรัสตัวหนึ่งอาจจะซ่อนอยู่ในโปรแกรมตารางคำนวณ แล้วไม่ทำอะไรนอกจากพอถึงการคำนวณครั้งที่ 50 ก็แกล้งให้ผิดเล็กน้อยและจึงรอไปจนถึงครั้งที่ 50 อีกก็แกล้งให้ผิดอีก

หรือไวรัสอาจจะแอบแฝงอยู่ในโปรแกรมประมวลผลคำ (WORD PROCESSING) เวลาพิมพ์จดหมายฉบับแรกก็ไม่ให้มีผิดเลย พอฉบับที่สองก็ให้มีผิด 1 ตัว พอฉบับที่สามก็ถูกหมดและฉบับที่สี่สั่งผิดอีก 1 ตัว โดยเป็นคนละตัวกับที่ผิดครั้งแรก แบบนี้ก็คงตรวจพบลำบากมาก

อีกแบบหนึ่งไวรัสอาจจะแกล้งเปลี่ยนความหมายของแป้นพิมพ์จากแป้นตัว A นาน ๆ ที พอกดตัว A ก็ให้กลายเป็นตัว E แบบนี้ก็ทำให้เข้าใจ

ผิดว่าแป้นพิมพ์เก่าชำรุดอาจจะต้องเปลี่ยนแป้นใหม่ ซึ่งก็จะไม่แก้ปัญหาเพราะไม่ใช่ปัญหาที่แป้นแต่เป็นที่ไวรัส

หรือไวรัสอาจจะคอยดูว่าสั่งให้ส่งข้อมูลเข้าจานแม่เหล็กไหน นาน ๆ ก็ส่งผิดจานเสียทีหนึ่งเช่นสั่งให้เข้า A ก็เข้า A บ้าง ไปเข้า B บ้าง คงตรวจพบยาก เป็นต้น

กรณีไหนที่น่าสงสัยว่าจะถูกไวรัสบุก

มีกรณีที่น่าจะสงสัยได้ว่าจะถูกไวรัสบุกดังต่อไปนี้

- เครื่องคอมพิวเตอร์เครื่องใดที่มีผู้ใช้ร่วมกันหลาย ๆ คนทำให้ไวรัสจากคนหนึ่งไปติดอีกคนได้
- ระบบคอมพิวเตอร์ที่ไม่มีการทำสำเนาสำรองหรือทำไม่สม่ำเสมอ ทำให้ตรวจสอบความยาวของโปรแกรมว่าเปลี่ยนไปหรือไม่ลำบาก
- เครือข่ายคอมพิวเตอร์ อาจจะได้ไวรัสจากเทอร์มินัลอื่น
- คอมพิวเตอร์ที่มีโมเด็มให้คนโทรศัพท์เชื่อมโยงเข้ามาได้ เช่น ธนาคารในสำนักงาน ไวรัสจากลูกค้าลงมาจะเข้าเครื่องธนาคารได้
- แผ่นซอฟต์แวร์ชิ้นใดที่มีการให้ยืมไปใช้กันได้หลาย ๆ คน ใครเอาไปใช้อาจจะเอาไปติดไวรัสมาด้วย
- มีการใช้แฟ้มข้อมูลร่วมกัน ผู้ใช้คนหนึ่งอาจจะเอาโปรแกรมที่มีไวรัสมาปล่อยไวรัสให้แฟ้มก็ได้
- มีการใช้โปรแกรมสำเร็จที่มีการคัดลอกมาโดยไม่ถูกกฎหมายอาจจะติดไวรัสมาด้วย
- มีการใช้ซอฟต์แวร์ที่คัดลอกกันอยู่ฟรี ๆ ซึ่งอาจจะมีไวรัสอยู่
- มีการใช้ซอฟต์แวร์ที่ไม่มีการทดสอบตรวจหาไวรัสก่อนการใช้
- ไม่มีการควบคุมการแก้ไขปรับปรุงซอฟต์แวร์ อาจมีมือดีหลอกว่าจะปรับปรุงแล้วเอาไวรัสแถมไว้ก็ได้
- ไม่มีการตรวจหาและป้องกันไวรัส

การแก้ไขเมื่อได้พบไวรัส

เมื่อได้พบว่ามีไวรัสอยู่ในระบบของเราการแก้ไขก็ไม่ยากอะไร นั่นคือจัดการลบไวรัสออกให้หมด หรือลบทุกอย่างทิ้งแล้วไปคัดลอกจากโปรแกรมสำรองที่ไม่มีไวรัสปนเปื้อนอยู่

การแก้ไขนี้ไม่ยาก แต่สิ่งที่ยากคือทำอย่างไรจึงจะไม่ให้ติดไวรัสอีก นั่นคือประเด็นสำคัญต่อไปคือการป้องกันไม่ให้ติดไวรัส

การป้องกันไวรัสบุก

ได้มีผู้เสนอมาตรการป้องกันมากมายหลายแบบ สรุปแล้วก็คล้าย ๆ หญิงสาวจะป้องกันไม่ให้ท้อง วิธีที่มั่นใจได้ร้อยเปอร์เซ็นต์ก็คือไม่ยุ่งเกี่ยวกับผู้ชายคนใดเลย แต่มักจะทำลำบาก นั่นคือถ้าเราไม่ต้องการให้คอมพิวเตอร์ของเราติดไวรัส เราก็ต้องไม่ยุ่งเกี่ยวกับคอมพิวเตอร์อื่น ๆ เลย คือไม่ยอมใช้คอมพิวเตอร์ของเราติดต่อกับเครือข่ายคอมพิวเตอร์ใด ไม่ยอมซื้อหรือเอาโปรแกรมใหม่มาใช้เลย ไม่ว่าจะได้ฟรีหรือจะซื้อก็ไม่เอาทั้งนั้น ไม่ยอมให้ใครมาซ่อมเครื่องเพราะเขาอาจจะเปลี่ยนชิฟให้มีไวรัสติดเข้าไปก็ได้ อะไรทำนองนั้น

ในทางปฏิบัติคงจะเลิกยุ่งเกี่ยวกับใครหมดคงไม่ได้ ฉะนั้นคงจะต้องยอมยุ่งเกี่ยวแต่ต้องจัดหามาตรการป้องกันดังตัวอย่างต่อไปนี้

- ควบคุมการใช้เครื่อง เช่น โดยมีการใช้รหัสและเลขที่บัญชี และให้เครื่องจดรายละเอียดไว้หมดว่าใครมาใช้ทำอะไรเมื่อใด เป็นการป้องกันผู้ไม่มีสิทธิ์มาแอบใช้เครื่อง
- จัดวางนโยบายและแนวทางในการใช้ซอฟต์แวร์ที่ไม่ได้มาตรฐานทั้งหลายเช่น ซอฟต์แวร์ที่ไม่ทราบแหล่งผลิต ซอฟต์แวร์จากบ้าน ซอฟต์แวร์ที่มีการแจกฟรีไม่ว่าจะเป็นแผ่นดิสเกตต์หรือจากเครือข่ายคอมพิวเตอร์ เป็นต้น อาจจะมีนโยบายว่าก่อนใช้ซอฟต์แวร์เหล่านั้นจะต้องจัดทำสำเนาซอฟต์แวร์อื่นไว้ทั้งหมด และต้องนำซอฟต์แวร์ที่ไม่ได้มาตรฐานนั้นไปตรวจสอบดูโดยละเอียดว่าติดเชื้ออยู่หรือไม่
- จัดวางนโยบายเกี่ยวกับการคัดลอกซอฟต์แวร์ ซึ่งบางแห่งก็ห้ามคัดลอกโดยเด็ดขาด บางแห่งก็อนุญาตให้คัดลอกได้แต่ก่อนคัดลอกต้องตรวจสอบต้นฉบับให้แน่ใจว่าไม่มีไวรัส
- บังคับการตรวจสอบซอฟต์แวร์ทุกชุดก่อนแจกจ่ายให้พนักงานหรือเจ้าหน้าที่ใช้ จะตรวจสอบเพียงต้นฉบับอย่างเดียวไม่ได้ ต้องตรวจสอบสำเนาทุกชุดก่อนที่จะแจกจ่ายสำเนานั้น
- จัดวางระเบียบการตรวจสอบทั้งซอฟต์แวร์และฮาร์ดแวร์เป็นระยะ ๆ ทั้งโดยประกาศล่วงหน้าและไม่ประกาศ เช่นว่า ประกาศว่าจะตรวจสอบทุก 3

เดือนแต่วันดีคืนดีก็เข้าไปตรวจสอบด้วย

- ป้องกันการแก้ไขแฟ้มโดยไม่ได้รับอนุญาต ทั้งนี้โดยอาจจะใช้โปรแกรมต่อต้านไวรัส หรือระบบแปลงรหัส ซึ่งอาจจะแปลงรหัสโปรแกรมทั้งหมดไม่ให้ผู้ไม่หวังดีทราบได้ว่าโปรแกรมและข้อมูลอะไรอยู่ที่ใด ทำให้แก้ไขยากเข้า

- จัดหาซอฟต์แวร์ป้องกันการแก้ไขแฟ้ม เช่น ป้องกันไม่ให้ผู้ใช้เขียนอะไรลงบนแฟ้ม คือให้อ่านได้อย่างเดียว และห้ามเขียน เป็นต้น

- จัดวางระบบการอนุมัติการแก้ไขและการตรวจสอบผลการแก้ไขโปรแกรม ใครจะแก้โปรแกรมอะไรต้องขออนุมัติเป็นลายลักษณ์อักษร เมื่อแก้แล้วต้องมีการตรวจสอบว่า การแก้นั้นไม่ได้มีการเติมไวรัสให้ทั้งโดยตั้งใจหรือไม่ตั้งใจ

- จัดประชาสัมพันธ์ให้พนักงานเจ้าหน้าที่และผู้เกี่ยวข้องทุกคนเห็นความสำคัญของการป้องกันไวรัส และร่วมมือร่วมใจกันปฏิบัติตามกฎระเบียบโดยเคร่งครัด

ซอฟต์แวร์ต่อต้านไวรัส

ในปัจจุบันมีผู้ผลิตซอฟต์แวร์ต่อต้านไวรัสมากมายในเมืองไทย ทั้งที่สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง และมหาวิทยาลัยอื่น ๆ ก็จัดทำโปรแกรมดังกล่าวขึ้น แต่ข้อสำคัญก็เหมือนกับยารักษาโรค ตัวยาตัวใดตัวหนึ่งก็มีสรรพคุณจำกัด ซอฟต์แวร์ต่อต้านไวรัสตัวใดตัวหนึ่งก็ต่อต้านได้เฉพาะไวรัสตัวนั้นเท่านั้น ในทำนองเดียวกับที่ไวรัสจริงอาจจะดื้อยาปรับปรุงตัวเองให้เก่งกล้าสามารถขึ้น ผู้สร้างไวรัสคอมพิวเตอร์ก็อาจจะปรับปรุงไวรัสให้เก่งกล้าสามารถขึ้นได้เป็นต้น

ท่านผู้อ่านคงจะรู้จักโปรแกรมต่อต้านไวรัสที่ผลิตขึ้นในเมืองไทยกันดีแล้ว ฉะนั้นในบทความนี้จะกล่าวถึงเฉพาะตัวอย่างโปรแกรมต่อต้านไวรัสจากต่างประเทศโดยเรียงลำดับตามตัวอักษร

- แอนติโดท (ANTIDOTE) ผลิตโดยบริษัทเควทซอฟต์แวร์ที่เมืองโตรอนโต แคนาดา ผู้ผลิตอ้างว่ามีคุณสมบัติป้องกันการติดเชื้อ คือป้องกันการแก้ไขแฟ้มที่มีอยู่แล้ว ทำให้ไวรัสคัดลอกตัวเองลงไปในแฟ้มอื่นไม่ได้

- ซีสี่ (C-4) และเรทโทรห้า (RETRO-V) จากบริษัทอินเตอร์พาร์ทที่แคลิฟอร์เนีย อ้างว่าสามารถป้องกันการติดเชื้อไวรัสที่มีผู้พบแล้ว 39 ชนิด

- คริปโตลอดที่สอง (CRYPTOLODE II) จากบริษัทคอมคริปต์ ที่แมรี่แลนด์ อ้างว่าเป็นโปรแกรมแปลงรหัสเพื่อป้องกันไวรัส

- หมอดาต้า (DATA PHYSICIAN) แอนติเจน (ANTIGEN) และไร้ไวรัส (NO VIRUS) จากบริษัทดิจิตัลดิสแพทช์ ในมินิอาโปลิส เจ้าหมอดาต้านั้นผู้ผลิตอ้างว่าคัดลอกทำสำเนาโปรแกรมทุกโปรแกรมและตรวจสอบเป็นระยะว่ามีการแก้ไขเปลี่ยนแปลงหรือไม่ ถ้าพบการแก้ไขก็จะสะกิดเจ้าของว่าสงสัยจะถูกไวรัส ส่วนเจ้าแอนติเจน จะทำตัวเป็นไวรัสแต่เป็นไวรัสผู้ทรงคุณธรรมเข้าเกาะโปรแกรมที่จะป้องกัน แล้วคอยดูว่าจะมีไวรัสจะมาเกาะหรือไม่ ถ้ามีก็โวยวายทันที ส่วนเจ้าไร้ไวรัสจะเข้าไปอยู่ในส่วนความจำของเครื่องทุกครั้งที่มีการเปิดเครื่องแล้วคอยเฝ้าระวังไม่ให้ไวรัสมาอาละวาด

- ผู้เฝ้าดิสก์ (DISK WATCHER) จาก อาร์จีซอฟต์แวร์ ที่เมืองเพนซิลเวเนีย ทำหน้าที่ป้องกันไวรัสบุกฮาร์ดดิสก์

- หมอแพนด้า (DR.PANDA) จากบริษัทแพนด้าซิสเต็ม ประกอบด้วยโปรแกรมสามโปรแกรม สำหรับป้องกันความเสียหายจากไวรัสสี่แบบคือ

1. การเปลี่ยนแปลงฟอร์แมตของฮาร์ดดิสก์ทีละน้อย

2. การเปลี่ยนฟอร์แมตหรือลบดิสก์ทั้งหมด

3. การแก้ไขบูตเซกเตอร์

4. การแก้ไขตารางจัดการส่วนความจำ

โปรแกรมแรกชื่อ ฟิสิคัล (PHYSICAL) จะเก็บโอเอสและบูตเซกเตอร์ที่สะอาดปราศจากไวรัสไว้ แล้วไปเปรียบเทียบกับโอเอสกับบูตเซกเตอร์ที่ใช้จริงเป็นระยะ ๆ ถ้าสงสัยไวรัสก็โวยวายทันที โปรแกรมที่สองชื่อ มอนิเตอร์ (MONITOR) เข้าไปอยู่ในส่วนความจำแล้วคอยตรวจสอบว่ามีอะไรน่าสงสัยคล้ายไวรัสหรือไม่ ส่วนโปรแกรมที่สามชื่อ แลบเทสต์ (LABTEST) สำหรับให้ผู้เชี่ยวชาญเอาไว้เรียกใช้ตรวจไวรัส

- ฟลูชอร์ตพลัส (FLU-SHOT PLUS) เป็นโปรแกรมจากเครือข่ายคอมพิวเซิร์ฟและเครือข่ายอื่น ๆ เขียนโดยคุณกรีนเบอร์ก (GREENBERG) จากบริษัทซอฟต์แวร์คอมเซฟต์

- ฟาวเดชันแวร์วัคซีน (FOUNDATION WARE VACCINE) จากบริษัทฟาวเดชันแวร์ ในโอไฮโอ

- อินเทอร์รอน (INTERON) สำหรับเครื่องแมคอินทอช และแจกฟรี แต่ขอให้ผู้ใช้บริจาคเงินให้ผู้เขียนบ้าง

- เมซวัคซีน (Mace Vaccine) จากบริษัทพอลเมซซอฟต์แวร์ ใช้ป้องกันแฟ้มระบบ ป้องกันบูตเซกเตอร์ และป้องกันตารางต่าง ๆ ของโปรแกรมระบบ

วัคซีนเนต (VACCINATE) ไซรินจ์ (SYRINGE) และเคนนารี (CANARY) จากบริษัทซอฟโค ในโคโลราโด เจ้าตัววัคซีนเนตเป็นไวรัสประเภทผู้ทรงคุณธรรมซึ่งเข้าไปเกาะโปรแกรมที่จะป้องกัน และใช้ไซรินจ์ฉีดยาป้องกันไวรัสให้โปรแกรมนั้น คอยดูว่ามีไวรัสบุกเมื่อไรก็โวยวายขึ้น ส่วนเคนนารีเป็นโปรแกรมมีไว้สำหรับใช้กับโปรแกรมที่สงสัยว่าจะติดเชื้อ

- วัคซีน (VACCINE) จากวีซีซอฟต์แวร์ ในไอโอวา ใช้สำหรับแมคอินทอช

- วัคซีน (VACCINE) แอนติโดท (ANTIDOTE) และ เช็คอัพ (CHECK-UP) จากเวิล์ดไวด์คาตา ในนิวยอร์ก

- ไวรัสอลาม (VIR ALARM) จากบริษัทเลเซอร์ทรีฟ ในนิวเจอร์ซี ใช้สำหรับตรวจสอบว่ามีไวรัสหรือไม่ และถ้าไม่มีก็ใช้โปรแกรมป้องกันได้

- ไวรัสอาร์เอกซ์ (VIRUS RX) จากบริษัทแอปเปิลคอมพิวเตอร์

- ไวรัสเซฟ (VIRUSAFE) จากบริษัทคอมเนต อยู่ในแรม (RAM) ทำหน้าที่ตรวจสอบโปรแกรมว่า สงสัยไวรัสหรือไม่

สรุป

ไวรัสคอมพิวเตอร์เป็นปัญหาใหญ่ที่จะอยู่กับเราไปอีกนาน ปัจจุบันได้มีการค้นพบไวรัสแล้วถึง 39 ตัว มีโปรแกรมต่อต้านไวรัสกว่า 30 โปรแกรม หลักการของไวรัสเป็นหลักการง่าย ๆ ในแง่ที่แบ่งเป็น 3 ส่วน คือส่วนคัดลอก ส่วนสะกิดให้ลงมือ และส่วนลงมือ แต่ละส่วนก็มีรูปแบบได้แตกต่างกันมากมายเช่น จะคัดลอกลงตรงไหน จะสะกิดอย่างไร จะลงมือทำอะไรเป็นต้น ฉะนั้นจึงอาจจะมีมือดีสร้างไวรัสขึ้นอีกเป็นพัน ๆ ตัว บางตัวอาจจะแอบแฝงอยู่เป็นปีแล้วจึงจะลุกขึ้นมาอาละวาด ถ้าอาละวาดรุนแรงก็จะถูกจับได้ทันที แต่ถ้าอาละวาดทีละนิด ๆ ค่อย ๆ กัดให้กร่อนไปเรื่อย ๆ กว่าจะถูกจับได้ก็อาจจะทำความเสียหายให้อย่างมากมายแล้ว

ถ้าเจ้าตัวผู้สร้างไวรัสไม่ใส่ชื่อที่อยู่ไว้ให้ เมื่อจับไวรัสได้แล้วก็อาจจะหาผู้สร้างไม่ได้ นั่นคือจะลงโทษอะไรใครไม่ได้

แม้จะจับตัวผู้สร้างไวรัสได้ ก็อาจจะหากฎหมายมาลงโทษไม่ได้ เช่น ตัวไวรัสนั้นคัดลอกโปรแกรมดี ๆ ให้ทุกคนจนไม่มีใครมีเนื้อที่เหลือจะทำงานได้ ถ้าจะลงโทษผู้สร้างไวรัส เขาอาจจะอ้างว่าสิ่งที่เขาทำก็เหมือนกับการให้ของขวัญ เขาไม่ได้ลบอะไรของใครทิ้งและไม่ได้แก้ไขโปรแกรมและข้อมูลของใคร เขาเอาของขวัญหรือโปรแกรมดี ๆ ที่มีประโยชน์มาให้ทั้งนั้นแต่เผอิญให้มากไปหน่อย แล้วผิดด้วยหรือ ฉะนั้นจึงอาจจะต้องแก้กฎหมายว่าการให้ของขวัญหรือการแจกโปรแกรมฟรีนั้น ถ้าก่อให้เกิดความเสียหายแก่ผู้รับก็ให้ถือว่าผิดกฎหมาย หรืออะไรทำนองนั้น แต่ก็ต้องระวังอีกว่า "ความเสียหาย" นั้นแปลว่าอะไร เดี๋ยวอาจจะมีใครเป็น "หัวหมอ" เอากฎหมายนี้ไปใช้กับใครก็ได้ ที่เอาของขวัญมาให้เขาแล้วเขาจะหาเรื่องก็อ้างว่าของขวัญนั้นทำความเสียหายให้เขา

สรุปแล้วเรื่องนี้เป็นหัวข้อใหม่ในด้านคอมพิวเตอร์ที่จะต้องวิเคราะห์วิจัยกันต่อไปได้อีกมากมาย อาจจะมีทฤษฎีไวรัส คณิตศาสตร์ไวรัส ระเบียบวิธีปฏิบัติการด้านไวรัส และกฎหมายเกี่ยวกับไวรัส เป็นต้น ชาวไทยคนไหนสนใจจะเล่นเรื่องไวรัสคอมพิวเตอร์ก็เชิญได้เลยครับ

บรรณานุกรม

1. Cohen, F. "Computer viruses: Theory and Experiments" in Computer and Security, V.6, No.1, February 1987. pp. 23-24.
2. Davis F.G. and Ganteinbein, R.E. "Recovering from a Computer Virus Attack," Journal of Systems & Software, V.7, No.4 (December, 1987), pp.253-58.
3. Gibson, S: "Computer Viruses Express Themselves in Many Ways," Inforworld. April 18, 1988.
4. Landburg, T: Computer Virused and Trojan Horses: A Guide to Protecting your Computer. National Bureau of Standard/Institute of Computer Science and Technology, Richmond, VA, USA, March 8, 1988.
5. Marbach, W.D: "Is your Computer Infected?" Newsweek, February 1, 1988.
6. Pozzo, M.M. and Gray, T.E: "An Approach to Containing of Computer Viruses." Computer & Security, V.6, N. 4 (August 1987), pp.321-31. Angeles, 1986.
7. Schoch, J.F. and Hupp, J.A: "The Worm Programs: Early Experience with a Distributed Computation," Communications of the ACM, V.25, No.3 (March 1982).
8. "Computer Systems Under Siege, Here and Abroad," New York Times, January 31, 1988.
9. "Computer 'Viruses' Turn Out to Be Serious Problem," Washington Post Writer's Group, May 3, 1988.